SOPHOS

sophos anti-virus

User manual

UNIX

For network and single computers

Document date: February 2007

About this manual

This user manual explains how to use Sophos Anti-Virus for UNIX and how to configure

- virus scanning
- quarantining of infected files
- disinfection
- central reporting.

The manual also provides help in resolving common problems and explains how to uninstall Sophos Anti-Virus from a UNIX server.

For information on *automatically* installing and updating Sophos Anti-Virus, see the *Sophos Anti-Virus and Sophos Client Firewall network startup guide* on the **Sophos Anti-Virus Network Install CD**. For information on *manually* installing and updating Sophos Anti-Virus, see the *Sophos Anti-Virus UNIX startup guide* on the **Sophos Anti-Virus Supplementary CD**.

Sophos documentation is published on the Sophos CDs and at www.sophos.com/support/docs/

Contents

Using Sophos Anti-Virus

1 Scanning the computer for viruses 6

2 Quarantining infected files 8

3 Disinfection 9

4 Error codes 11

Configuration

5 Configuring Sophos Anti-Virus 14

6 Command line options 16

Central reporting

7 Starting and monitoring central reporting 26

8 Configuring central reporting 28

9 Setting central reporting levels 30

Troubleshooting

10 Troubleshooting 34

Appendix

Appendix 1 Uninstalling Sophos Anti-Virus 40

Glossary and index

Glossary 42

Index 45

Technical support 47

Using Sophos Anti-Virus

Scanning the computer for viruses

Quarantining infected files

Disinfection

Error codes

1 Scanning the computer for viruses

To scan items for viruses, enter the command ‘sweep’ followed by the path of the items to be scanned.

By default, Sophos Anti-Virus scans

- executable Windows files
- .sh and .pl files
- files that can contain macros
- HTML files
- files compressed with PKLite, LZEXE and Diet
- directories below the one specified
- items pointed to by symbolic links.

For a full list of the file types scanned, run sweep with the -vv option.

For information on changing these settings, see sections 5 and 6.

Sophos Anti-Virus can scan UNIX computers at set times automatically. This is done using the crontab facility. See the documentation for your system.

1.1 Scanning the local computer

To scan the local computer, enter

```
sweep /
```

1.2 Scanning a particular directory or file

To scan a particular directory or file, use the path of the item to be scanned, for example

```
sweep /usr/mydirectory/myfile
```

1.3 Scanning a filesystem

To scan a filesystem, use the name of the filesystem, for example

```
sweep /home
```

More than one filesystem can be entered in the command line.

1.4 Scanning a boot sector

Boot sector scanning is available only for Linux/Intel (libc6) and FreeBSD (versions 3 and later).

You can scan boot sectors of logical and physical drives.

To scan boot sectors, log in as superuser (to get sufficient permission to access the disk devices) and then use one of the commands shown below.

To scan the boot sectors of specified logical drives, enter

```
sweep -bs=xxx, xxx,...
```

where xxx is the name of a drive (for example /dev/fd0 or /dev/hda1).

To scan boot sectors for all logical drives that Sophos Anti-Virus recognises, enter

```
sweep -bs
```

To scan the master boot records for all the fixed physical drives on the system, enter

```
sweep -mbr
```

1.5 Finding a virus

After the scan, you will see a message similar to that shown below.

If Sophos Anti-Virus has found a virus, it reports it in the line which starts with >>> and is followed by either `Virus` or `Virus fragment`.

```
SWEEP virus detection utility
Version 3.90.0 [Linux/Intel]
Virus data version 3.90, February 2005
Includes detection for 99603 viruses, trojans and worms
Copyright (c) 1989-2005 Sophos Plc, www.sophos.com

System time 09:35:55, System date 16 February 2005

Quick Sweeping

>>> Virus 'EICAR-AV-Test' found in file /home/source/eicar.src

33 files swept in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com, email support@sophos.com
or telephone +44 1235 559933
End of Sweep.
```

For information on disinfection, see section 3.

2 Quarantining infected files

You can configure Sophos Anti-Virus to put infected files into quarantine (i.e. to prevent them from being accessed). It does this by changing the ownership and permissions for the file.

To specify quarantining, enter

```
sweep PATH --quarantine
```

where PATH is the path to be scanned.

By default, Sophos Anti-Virus changes the ownership of an infected file to that of the user running Sophos Anti-Virus and changes the file permissions to -r-------- (0400).

If you prefer, you can specify the user or group ownership and file permissions that Sophos will apply to infected files. You do so by using the parameters

```
<uid=nnn>
<user=username>
<gid=nnn>
<group=groupname>
<mode=ppp>
```

You cannot specify more than one parameter of each type, e.g. you cannot enter the same username twice, or enter a uid and a username.

For each parameter you do not specify, the default setting (as given above) is used.

For example:

```
sweep fred --quarantine:user=sweep,group=virus,mode=0400
```

will change an infected file's user ownership to sweep, the group ownership to virus, and the file permissions to -r--------.

If you specify disinfection (see section 3) as well as quarantining, Sophos Anti-Virus attempts to disinfect infected items and quarantines them only if disinfection fails.

3 Disinfection

This section describes how to disinfect infected items on a UNIX computer. For information on disinfecting non-UNIX workstations, see the Sophos Anti-Virus documentation for that platform.

The method you use depends on whether you want to disinfect a data file, a program, or a boot sector.

3.1 To disinfect a data file

To disinfect a specific data file (e.g. a document or spreadsheet), enter

```
sweep [data file path] -di
```

Alternatively, to detect and remove viruses in any data file or program on the system, enter

```
sweep / -di
```

In either case, Sophos Anti-Virus asks for confirmation before it disinfects.

Check the data file(s) carefully afterwards. Sophos Anti-Virus can remove the virus, but cannot reverse any side-effects. Check the analysis of the virus on the Sophos website for information about its possible side-effects.

3.2 To disinfect a Windows program

You can eliminate viruses in program files in two ways.

To disinfect a program file, enter

```
sweep [program filename] -di
```

This ensures that the virus cannot spread. However, the program file may be corrupted. You should subsequently delete it and replace it from a backup.

To remove an infected program file, enter

```
sweep [program filename] -remove
```

Alternatively, to remove all infected programs, enter

```
sweep / -remove
```

In either case, Sophos Anti-Virus asks for confirmation before it removes the program(s).

3.3 To disinfect a boot sector

Boot sector disinfection is available only for Linux/Intel (libc6) and FreeBSD (versions 3 and later).

To disinfect a boot sector, enter

```
sweep -bs=xxx -di
```

where `xxx` is the name of a drive.

For example, to eliminate a virus in the floppy drive

```
sweep -bs=/dev/fd0 -di
```

4 Error codes

Sophos Anti-Virus returns error codes if there is an error or if a virus is found.

0 If no errors are encountered and no viruses are found.

1 If the user interrupts the execution by pressing 'Ctrl'+'c'.

2 If some error preventing further execution is discovered.

3 If viruses or virus fragments are discovered.

4.1 Extended error codes

A different set of error codes are returned if the sweep command is run with the -eec qualifier.

0 If no errors are encountered and no viruses are found.

8 If survivable errors have occurred.

16 If password-protected files have been found. (They are not scanned.)

20 If viruses have been found and disinfected.

24 If viruses have been found and not disinfected.

28 If viruses have been found in memory.

32 If there has been an integrity check failure.

36 If unsurvivable errors have occurred.

40 If execution has been interrupted.

Configuration

Configuring Sophos Anti-Virus

Command line options

5 Configuring Sophos Anti-Virus

This section describes how to configure Sophos Anti-Virus to

- scan all file types (section 5.1)
- scan inside archives (section 5.2)
- scan remote computers (section 5.3)
- avoid scanning symbolically linked items (section 5.4)
- scan the starting filesystem or computer only (section 5.5).

For a full list of the configuration options, see section 6.

In this section, where PATH appears in a command, it refers to the path to be scanned.

5.1 Scanning all file types

By default, Sophos Anti-Virus scans executable files only. To scan all files, irrespective of their type, enter

```
sweep PATH -all
```

This takes longer than scanning only executables, and can compromise performance on servers. It can also cause false virus reports.

5.2 Scanning inside archives

Sophos Anti-Virus can scan inside archives if it is run with the -archive option

```
sweep PATH -archive
```

Archive types that can be scanned include: ARJ, CMZ, GZip, RAR, TAR, Zip.

Archives 'nested' within other archives (e.g. a TAR archive within a Zip archive) are scanned recursively.

Alternatively, you can specify scanning of particular types of archive. For example, to scan inside TAR archives, enter

```
sweep PATH -tar
```

or to scan inside TAR and Zip archives, enter

```
sweep PATH -tar -zip
```

If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

For a full list of the archive types scanned, use the -vv option.

5.3 Scanning remote computers

By default, Sophos Anti-Virus does not scan items on remote computers (i.e. does not traverse remote mount points). To enable scanning of remote computers, enter

```
sweep PATH --no-stay-on-machine
```

5.4 Disabling scanning of symbolically linked items

By default, Sophos Anti-Virus scans symbolically linked items. To disable this type of scanning, enter

```
sweep PATH --no-follow-symlinks
```

To avoid scanning items more than once, use the --backtrack-protection option.

5.5 Scanning the starting filesystem only

Sophos Anti-Virus can be configured not to scan items that are beyond the starting filesystem (i.e. not to traverse mount points). Enter

```
sweep PATH --stay-on-filesystem
```

6 Command line options

The command line options listed in this section enable you to configure scanning and disinfection. There are

- options that Sophos Anti-Virus for UNIX has in common with other versions of Sophos Anti-Virus (section 6.1)
- options specific to Sophos Anti-Virus for UNIX (section 6.2)
- options specific to Linux and FreeBSD (section 6.3).

In this section, where PATH appears in a command, it refers to the path to be scanned.

6.1 Sophos Anti-Virus command line options

To invert the meaning of a command line option, prefix it with 'n'. For example, -nsc is the inverse of -sc.

For a listing of these options on screen, enter

```
sweep -h
```

-all Scan all files

If this option is used, Sophos Anti-Virus will scan all files in a filesystem, rather than just the executable files.

This takes longer than scanning executables only and can compromise performance on servers. It can also cause false virus reports.

-archive Scan inside archives

If this option is used, Sophos Anti-Virus scans inside archives. The archive types scanned include ARJ, CMZ, GZip, RAR, TAR, Zip.

Archives 'nested' within other archives (e.g. a TAR archive within a Zip archive) are scanned recursively.

Alternatively, you can specify scanning of particular types of archive. For example, to scan inside TAR archives, enter

```
sweep PATH -tar
```

or to scan inside TAR and Zip archives, enter

```
sweep PATH -tar -zip
```

If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

For a full list of the archive types scanned, use the -vv option.

-b Sound bell on virus detection

This option directs Sophos Anti-Virus to sound a bell when a virus or virus fragment is discovered. It is enabled by default.

-c Ask for confirmation before disinfection or deletion

This option directs Sophos Anti-Virus to ask for confirmation before disinfecting or deleting files. It is enabled by default.

-di Disinfect

This option enables Sophos Anti-Virus to perform automatic disinfection of data files, programs and boot sectors. See section 3.

-dn Display names of files as they are scanned

This option displays files being scanned. The display consists of the time followed by the item being checked.

-eec Use extended set of error codes

This option directs Sophos Anti-Virus to use an extended set of error codes. For details, see section 4.

-exclude Exclude items from scanning

This option enables you to specify that any items (files, directories or filesystems) that follow the option on the command line must be excluded from scanning.

After using the option -exclude, you can use the option -include to specify that items that follow this option on the command line must be scanned.

For example

```
sweep fred harry -exclude tom peter -include bill
```

scans items fred, harry and bill, but not tom or peter.

The option -exclude can be used for files or directories under another directory. For example

```
sweep /home/fred -exclude /home/fred/games
```

scans all of Fred's home directory, but excludes the directory games (and all directories and files under it).

-ext= File types defined as executables

By default, Sophos Anti-Virus scans DOS and Windows executable files with certain file extensions (run sweep with the -vv qualifier to see a list of the file extensions used).

To specify additional file extensions that Sophos Anti-Virus will scan, use the -ext= option with a comma-separated list of extensions.

To exempt file extensions from scanning, use -next.

If you want to scan files that UNIX defines as executables, see the examine-x-bit qualifier in section 6.2.

-f Full scan

By default, Sophos Anti-Virus checks only those parts of each file that are likely to contain viruses. A 'full' scan examines the complete contents of each file and can be specified using this option.

Full scanning is slower than default scanning.

-h Help

This option lists all the command line options, including UNIX-specific options.

-idedir= Use alternative directory for virus identity files (IDEs)

This option enables you to specify an alternative directory for IDEs. For example

```
sweep PATH -idedir=/ide
```

directs Sophos Anti-Virus to read IDEs from the `/ide` directory instead of the default directory (normally `/usr/local/sav`).

-mime Scan MIME files

This option enables Sophos Anti-Virus to scan MIME files when it does a scan. By default, it is ***not*** enabled to scan MIME files.

--no-stop-scan Scan files that Sophos Anti-Virus incorrectly identifies as "zip bombs"

By default, Sophos Anti-Virus stops scanning "zip bombs" when they are detected.

? "Zip bombs" are malicious files that are designed to disrupt the action of anti-virus scanners. These files usually take the form of innocent looking archive files that, when unpacked in order to be scanned, require enormous amounts of time, disk space, or memory.

When a "zip bomb" is detected, a message such as

```
Aborted checking /home/fred/misc/b.zip - appears to be a 'zip bomb'
```

is displayed. Occasionally, Sophos Anti-Virus incorrectly identifies files that have complex and/or multiple levels of archiving as "zip bombs", and stops scanning them. To scan such files, rescan them using the option --no-stop-scan. For example

```
sweep /home/fred/package.zip --no-stop-scan
```

directs Sophos Anti-Virus to scan package.zip, even if it identifies it as a "zip bomb".

! Use this option only if absolutely necessary. If a genuine "zip bomb" is accessed with this option, Sophos Anti-Virus continues to scan it.

-oe Scan Outlook Express mailboxes

This option directs Sophos Anti-Virus to scan Outlook Express mailboxes when it does a scan. By default, it is ***not*** enabled to scan Outlook Express mailboxes. You must also use the -mime option with this qualifier.

-p=<file|device> Copy screen output to file or device

This option directs Sophos Anti-Virus to send whatever it sends to the screen to a particular file or device as well. For example

```
sweep PATH -p=log.txt
```

directs Sophos Anti-Virus to send screen output to the file log.txt.

-rec Do recursive scan

This option directs Sophos Anti-Virus to scan directories below the ones specified in the command line. It is enabled by default.

-remove Remove infected objects

This option directs Sophos Anti-Virus to remove infected items.

-s Silent running without displaying checked areas

If this option is used, Sophos Anti-Virus does not display on the screen the files it is scanning. It is enabled by default.

-sc Scan inside compressed files

If this option is used, Sophos Anti-Virus looks for viruses inside files compressed with PKLite, LZEXE and Diet. It is enabled by default.

-v Version number

If this option is used, Sophos Anti-Virus displays the version number and a list of the virus identities (IDEs) currently in use.

-vv Full version information

If this option is used, Sophos Anti-Virus displays the version number and lists of the virus identities (IDEs) currently in use, the file extensions that are scanned, and the archive types scanned.

6.2 UNIX-specific command line options

The following options are UNIX-specific, and may be prefixed with 'no-' to invert their meaning.

For example, '--no-follow-symlinks' is the inverse of '--follow-symlinks'.

--args-file=[filename] Read command line arguments from file

Sophos Anti-Virus reads command line arguments from a file. The arguments may include (lists of) directory names, filenames and options. For example

```
sweep --args-file=scanlist
```

directs Sophos Anti-Virus to read command line arguments from the `scanlist` file. When Sophos Anti-Virus reaches the end of the file, it continues reading arguments from the command line.

If [filename] is '-', Sophos Anti-Virus reads arguments from stdin. Some command line options may not be used in the file: -eec, -neec, -p=, -s, -ns, -dn and -ndn.

The backslash character is treated in a similar way to how it is in the UNIX shell (i.e. as a special prefix character). This enables you to specify filenames that contain unusual characters. The following rules apply:

- A backslash followed by another character generally means that that character is to be used literally (e.g. \" means a double quote).
- A backslash followed by another backslash means a single backslash.
- A backslash followed by certain letters means a control code (e.g. \n means new line, \t means tab, \r means carriage return, etc.).

- A backslash followed by an octal code means the character that corresponds to that code (e.g. \145 means the letter e, \40 means the space character, etc.). Octal codes can be 1 to 3 octal digits, but note that a non-octal digit terminates the code.

--backtrack-protection Prevent backtracking

Sophos Anti-Virus avoids scanning the same files more than once ('backtracking'), a problem that can arise due to symbolic links. This option is enabled by default.

--examine-x-bit Scan all items that UNIX defines as executables

If this option is used, Sophos Anti-Virus scans all items that UNIX defines as executables, as well as items with the file extensions in Sophos Anti-Virus's own executables list (for details of the file extensions listed, run sweep with the -vv qualifier). This option is disabled by default.

--follow-symlinks Scan the object pointed to by symbolic links

Sophos Anti-Virus scans objects pointed to by symbolic links. This option is enabled by default.

--preserve-backtrack Preserve backtracking information

Sophos Anti-Virus preserves the backtracking information for the duration of the run. This option is enabled by default.

--quarantine Quarantine infected files

If this option is used, Sophos Anti-Virus puts infected files into quarantine. Sophos Anti-Virus does this by changing the ownership and permissions for the file.

If you have specified disinfection, Sophos Anti-Virus attempts to disinfect the file and quarantines the file only if disinfection fails.

Unless you specify otherwise, Sophos Anti-Virus changes the ownership of the file to that of the user running Sophos Anti-Virus and changes the file permissions to -r -------- (0400).

You can use the option with further parameters:

```
<uid=nnn>
<user=username>
<gid=nnn>
<group=groupname>
<mode=ppp>
```

You cannot specify more than one parameter of each type (e.g. you cannot enter username twice, or enter a uid and a username).

For each parameter you do not specify, the default setting is used.

For example:

```
sweep fred --quarantine:user=sweep,group=virus,mode=0400
```

changes an infected file's user ownership to sweep, the group ownership to virus, and the file permissions to -r--------.

You may need to be running as a special user or as superuser to set the ownership and permissions.

--reset-atime Reset the access time on files

After Sophos Anti-Virus scans a file, it resets the access time (the atime) to the time shown before scanning. However, if a file is disinfected, the access and modification times are updated. This option is enabled by default.

You may find that your archiver always backs up all the files that have been scanned. This could happen because resetting the atime has the effect of changing the inode status-changed time (ctime). In this case, run sweep with the --no-reset-atime option.

--show-file-details Show details of file ownership

If this option is used, Sophos Anti-Virus shows details of the file ownership and permissions when filenames are displayed or written to a log.

--skip-special Do not scan 'special' objects

Sophos Anti-Virus does not scan special objects, such as /dev, /proc, /devices etc. This option is enabled by default.

--stay-on-filesystem Do not leave the starting filesystem

If this option is used, Sophos Anti-Virus scans only the starting filesystem, i.e. it does not traverse mount points.

--stay-on-machine Do not leave the starting computer

Sophos Anti-Virus scans only the starting computer, i.e. it does not traverse remote mount points. This option is enabled by default.

6.3 Linux and FreeBSD-specific command line options

The following boot sector scanning options are only available with Sophos Anti-Virus for Linux (Libc6) and Sophos Anti-Virus for FreeBSD (versions 3 and later).

-bs=xxx, xxx,... Scan boot sector of specific logical drive

Sophos Anti-Virus scans the boot sectors of specified logical drives, where xxx is the name of the drive (for example /dev/fd0 or /dev/hda1). The floppy drive is considered a logical device for the purposes of this option.

You can use this option to scan the boot sectors of floppy disks that were created for other operating systems (e.g. Windows and DOS).

-bs Scan all known boot sectors

Sophos Anti-Virus extracts partition table information from all the physical drives it knows about, then scans all logical drive boot sectors. This includes boot sectors that are not Linux or FreeBSD (e.g. Windows and DOS).

-cdr= Scan CD boot image

To scan the boot image of a bootable CD, use the -cdr option. For example

```
sweep -cdr=/dev/cdrom
```

scans the boot image (if any) of the CD on device /dev/cdrom. If Sophos Anti-Virus finds a boot image, it scans the boot sector of that image for boot sector viruses.

To scan for program viruses all files in the boot image whose file type is in Sophos Anti-Virus's own executables list, use the -loopback option. For example

```
sweep -cdr=/dev/cdrom -loopback
```

scans the boot image (if any) of the CD on device /dev/cdrom. If Sophos Anti-Virus finds a boot image, it scans the boot sector of that image for boot sector viruses and scans for program viruses all files in that image whose file type is in the executables list.

-mbr Scan master boot records

Sophos Anti-Virus attempts to scan the master boot records for all the physical drives on the system.

Central reporting

Starting and monitoring central reporting

Configuring central reporting

Setting central reporting levels

7 Starting and monitoring central reporting

If you installed InterCheck Server, Windows workstations on your network can send virus reports to a central location.

By default, the directory used is `/var/spool/intercheck`.

The `/var/spool/intercheck` directory must be an exported directory visible to non-UNIX workstations running InterCheck. It has two subdirectories: `infected` and `comms`. Both are owned by user and group `sweep`. `infected` has permissions 0700 and `comms` has permissions 1777.

This section tells you how to

- start InterCheck Server
- stop InterCheck Server
- monitor InterCheck Server activity.

7.1 Starting InterCheck Server

When InterCheck Server is installed for the first time, or if it has been shut down, you start it by entering

```
icheckd
```

You can use the following options with this command:

-d

Run as a daemon (this is the default and recommended mode).

-nd

Do not run as a daemon. This will cause InterCheck to run in the foreground, and all logging information will be sent to the screen.

-c filename

Specifies the configuration file to use. Default is `/etc/icheckd.conf`.

-h

Displays usage information.

When InterCheck Server starts, it runs with default settings, unless you have created a configuration file (see section 8).

You can stop and restart InterCheck Server by sending a SIGHUP signal to it.

7.2 Stopping InterCheck Server

To stop InterCheck Server, enter

```
icheckd -stop
```

7.3 Monitoring InterCheck Server

To monitor InterCheck Server, look in the file

```
sweepic.res
```

The file contains statistics and details of InterCheck Server activity.

The default location for this file is `/var/spool/intercheck/comms`.

The sweepic.res file contains raw statistics. If you want to make the information more accessible, you can write a script to process the file.

8 Configuring central reporting

To change the settings that InterCheck Server uses, set up a configuration file called /etc/icheckd.conf and type in the parameters listed in section 8.1. For a sample file, see section 8.2.

InterCheck Server reads the settings from this file each time it starts up.

If you want InterCheck Server to use the new settings straight away, send it a SIGHUP signal (or stop and start it, as described in section 7).

8.1 InterCheck Server configuration options

The following configuration options are available:

EmailCmd=<String>

Specifies the name of the mailer program used to send mail to users when a workstation detects a virus, or when the filesystem is full.

Email is disabled by setting this option (or EmailRecipient) to nothing, for example

```
EmailCmd=
```

The default is `/bin/mail`.

EmailLevel=<number>

Specifies the reporting level above which users are sent email when a virus is detected, or when the filesystem is full.

See section 9 for information on the reporting level and how it is set.

If the email level is higher than the reporting level, e.g. if the reporting level is VIRUS (or 2) and the email level is INFORMATION (or 5), no email is sent.

The default is 0, i.e. mail is always sent.

EmailRecipient=<String>

Specifies the name of a user to whom email is sent either when a virus is detected, or if the filesystem is full.

Email is disabled by setting this option or EmailCmd to nothing, e.g.

```
EmailRecipient=
```

The default is sweep.

LogFacility=<string>

Enables you to specify the syslog facility to use when logging information. The facility may be: daemon, local 0, local 1 ... local7.

The default is daemon.

Rootdirectory=<String>

This option is used to specify the name of InterCheck Server's root directory. The comms and infected directories are found here, as is the lists directory if installing for diskless workstations.

The default is `/var/spool/intercheck`.

8.2 Sample configuration file

A sample configuration file might be as follows:

```
RootDirectory=/var/spool/intercheck
EmailRecipient=sysadmin
EmailCmd=/bin/mail
```

9 Setting central reporting levels

Since InterCheck Server runs as a daemon process, reporting information is returned via the UNIX syslog facility.

To change the level of events reported by InterCheck Server to the UNIX syslog, open the file

```
sweepic.ini
```

and edit the field

```
Reporting Level =
```

By default, the file sweepic.ini is in the directory /var/spool/intercheck/comms.

The level of reporting ranges from NONE (no reporting) to VERBOSE (verbose reporting). At VERBOSE level, details of every file which has been scanned are logged. For information about viruses to be logged, a level of at least VIRUS must be set.

If the reporting level is set directly, it is represented as a number (from 0 to 6) rather than a word. For details, see section 9.1 below.

At higher reporting levels, the log file may fill up rapidly. InterCheck sends a warning (by mail) if the filesystem is filling up, but you should regularly check whether this is happening, and empty the log file if necessary.

The default reporting level is VIRUS.

9.1 Reporting level and UNIX log level

The correspondence between the reporting level and the UNIX log level is as follows.

Reporting Level	UNIX log level
NONE (or 0)	n/a
FATAL (or 1)	LOG_CRIT
VIRUS (or 2)	LOG_CRIT
ERROR (or 3)	LOG_ERR
WARNING (or 4)	LOG_WARNING
INFORMATION (or 5)	LOG_INFO
VERBOSE (or 6)	LOG_NOTICE

Depending on the version of UNIX, reporting information from InterCheck may be enabled by including a line similar to the following in the syslog configuration file (usually /etc/syslog.conf):

```
daemon.notice        /var/log/daemon
```

There may already be a line similar to this in the syslog configuration file.

The name of the file to which reporting information is sent varies according to the system and the user's preferences/requirements.

It is also possible to alter the syslog facility from its default setting of daemon by using the LogFacility option in /etc/icheckd.conf.

The level of reporting information can be limited by one or both of the following

- The InterCheck reporting level (see above)
- The reporting level set in the configuration file (see section 8.1).

For further information about system logging and the system log file, consult your system manuals.

Troubleshooting

10 Troubleshooting

This section provides answers to some common problems that you may encounter when using Sophos Anti-Virus for UNIX. (For more information about Sophos Anti-Virus for UNIX error codes, see section 4.)

If your problem is not described in this section, refer to the Sophos website www.sophos.com which includes a support knowledgebase, virus analyses, the latest IDEs, product downloads and technical articles.

If your problem is not described on the website, contact Sophos technical support.

10.1 System reports 'not found' or 'cannot load library'

If the system returns either of these messages when you try to run Sophos Anti-Virus, you probably need to change your system settings. Ensure that the environment variables in your login script or profile include the directories that Sophos Anti-Virus uses.

- `PATH` should include `/usr/local/bin`
- `MANPATH` should include `/usr/local/man`
- `LD_LIBRARY_PATH` should include `/usr/local/lib.`

In AIX, the library environment variable is `LIBPATH`, and in HPUX it is `SHLIB_PATH`.

On some systems, such as FreeBSD and Linux, you can enable Sophos Anti-Virus to use the Sophos Anti-Virus shared libraries by running ldconfig. This may require editing of `/etc/ld.so.conf`.

If any of these variables are not included, add them to the environment variable(s) as shown in the examples below. Do not alter any of the existing settings.

If you are running the sh, ksh or bash shell, enter

```
PATH=$PATH:/usr/local/bin
export PATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
```

If you are running the csh or tsh shell, enter

```
setenv PATH [values]:/usr/local/bin
setenv LD_LIBRARY_PATH [values]:/usr/local/lib
```

where `[values]` are the existing settings.

You should make these variables system-wide. To do this, amend `/etc/login` or `/etc/profile`.

If you ***do not*** have a login script, you will need to reset these values every time you restart the server.

10.2 Sophos Anti-Virus runs out of disk space

This problem may arise when scanning complex archive files.

When it unpacks archive files, Sophos Anti-Virus uses the /tmp directory to store its working results. If this directory is not very large, Sophos Anti-Virus may run out of disk space. Specific users may encounter the same problem if Sophos Anti-Virus exceeds their disk size limit.

The solution is to enlarge /tmp or increase the users' disk size limit. Alternatively, change the directory Sophos Anti-Virus uses for working results. You can do this by setting the environment variable SAV_TMP.

10.3 Scanning runs slowly

Full scan

By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files likely to contain viruses. However, if scanning is set to full, it scans everything, and takes significantly longer to carry out a scan.

See the -f option in section 6.1.

Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).

Scanning all files

By default, Sophos Anti-Virus checks only files defined as executables. If it is configured to check all files the process takes longer. If you would like to scan other specific extensions, as well as executable files, add those extensions to the list of extensions Sophos Anti-Virus defines as executables.

See the -all and -ext= options in section 6.1.

10.4 Archiver backs up all files that have been scanned

Your archiver may always back up all the files that Sophos Anti-Virus has scanned. This can happen due to changes that Sophos Anti-Virus makes in the 'status-changed' time of files.

By default, Sophos Anti-Virus attempts to reset the access time (atime) of files to the time shown before scanning. However, this has the effect of changing the inode status-changed time (ctime). If your archiver uses the ctime to decide whether a file has changed, it backs up all files scanned by Sophos Anti-Virus.

To prevent such backups, run the sweep command with the --no-reset-atime qualifier.

10.5 InterCheck Server generates no information in the system log

There are several reasons why InterCheck Server may fail to generate syslog information.

InterCheck Server is not running

Use the ps command to look at the list of running processes, grepping for "icheckd". If InterCheck Server does not seem to be running, start it, as described in section 7.

Reporting is set to too low a level

The default level is VIRUS, which means that only virus alerts and fatal errors are logged to syslog. If the level is set to NONE, no messages are logged. If reporting levels are too low, InterCheck Server fails to generate syslog information. For details, see section 9.

Syslog configuration file is not set up properly

The syslog configuration file should specify where to send InterCheck Server log messages and specify messages of a high enough level. See section 7.

The system log file is full

The system log file may be so full that there is no more room on the filesystem. This may prevent InterCheck Server from working properly and may also prevent the system logging from working.

10.6 Virus fragment reported

If a virus fragment is reported, contact Sophos technical support for advice.

The report of a virus fragment indicates that part of a file matches part of a virus. There are three possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active.

Corrupted virus

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread.

Database containing a virus

When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file.

Appendix

Uninstalling Sophos Anti-Virus

Appendix 1 Uninstalling Sophos Anti-Virus

To uninstall Sophos Anti-Virus from the server, do as follows:

1. Ensure you are logged on to the server with root privileges or are superuser.
2. In `/usr/local/bin` delete

   `sweep`

   `icheckd`
3. In `/usr/local/lib` delete

   `libsavi.so*`
4. In `/usr/local/man` delete

   `icheckd.1`

   `icheckd.conf.5`

   `sweep.1`
5. Delete

   `/tmp/sav-install`

   `/usr/local/sav`
6. If you installed Sophos Anti-Virus on workstations connected to the server, delete the `InterChk` shared directory that you created on the server.
7. If your installation included InterCheck Server, delete

   `/var/spool/intercheck`

   You have uninstalled Sophos Anti-Virus from the server.

Glossary and index

Glossary

Boot sector: The first part of the operating system to be read into memory when a computer is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.

Boot sector virus: A type of virus that subverts the initial stages of the booting process. A boot sector virus attacks either the master boot sector or the DOS boot sector.

Central installation directory: See CID.

Checksum: A value calculated from item(s) of data. InterCheck creates a list of checksums of the files on the computer. If the checksum of a file is found to have changed, it is sent for scanning because it may have become infected with a virus.

CID: Central installation directory; a central location on a network from which Sophos Anti-Virus is installed and updated. You must install a different CID for each platform, and remember to keep every CID up to date.

Daemon: A process that runs in the background (i.e. independently of any user) with no input from or output to a terminal.

Executables: By default, Sophos Anti-Virus scans only files it defines as executables (even when full scanning is enabled). It is possible to: configure Sophos Anti-Virus to scan all files that *UNIX* defines as executables; configure Sophos Anti-Virus to scan all files; and to change the list of files defined as executables. Refer to sections 6.1 and 6.2.

Full scan: If configured to perform full scanning, Sophos Anti-Virus scans all files and all parts of files in the area it has been configured to scan. A full scan takes significantly longer than a quick scan. It is

	occasionally necessary in order to locate certain viruses. See section 6.1.
IDE:	Virus identity file; a type of file that contains the data Sophos Anti-Virus needs to enable it to detect a specific virus. IDEs are issued in between monthly updates to keep Sophos Anti-Virus up to date with the very latest viruses. IDEs should not be used to replace monthly updates.
Immediate scan:	A virus scan that is triggered by the user. It is possible to configure what is scanned, how it is scanned and what action should be taken if a virus is found.
InterCheck/InterCheck Client:	A component of Sophos Anti-Virus that intercepts files as they are accessed, and uses checksumming to determine whether or not they should be sent for virus scanning. It does not apply to **UNIX** computers.
InterCheck Server:	A component of Sophos Anti-Virus that enables workstations to send virus alerts to a central location.
Macro virus:	A type of virus that uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.
Master boot sector:	The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the computer is switched on (booted). It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition.
Mount point:	The point on a filesystem at which there is a transparent link to an item or items on another filesystem on the same computer. See also Symbolic link.
Quick scan:	The default scan type. Sophos Anti-Virus scans only the parts of files that can potentially contain executable code.

Remote mount point: The point on a filesystem at which there is a transparent link to an item or items on another filesystem on a remote computer. See also Symbolic link.

sweep: A component of Sophos Anti-Virus that carries out immediate and scheduled scanning.

Symbolic link: A link to a file or directory on another filesystem or another computer.

Syslog: A facility that logs system messages (e.g. messages from a daemon). See also Daemon.

Trojan horse: A computer program which carries out hidden and harmful functions. Generally Trojan horses trick the user into running them by claiming to have legitimate functionality. Backdoor Trojans enable other users to take control of your computer over the internet.

VDL: Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically.

Virus: A computer program that can spread across computers and networks by attaching itself to a program (such as a macro or boot sector) and making copies of itself.

Virus identity file: See IDE.

Worm: A type of virus that doesn't need a carrier program in order to replicate. Worms replicate themselves then use communications between computers (e.g. email programs) to spread.

Index

A

archives
  scanning 14, 16

B

backtracking
  preserving information 21
  preventing 21
backups of scanned files 36
boot image, CD 23
boot sector
  scanning 7

C

'cannot load library' message 34
CD boot image 23
central virus reporting
  configuring 28–29
  levels 31
  monitoring 27
  reporting levels 30–31
  starting 26
  stopping 27
command line options 20
compressed files
  scanning 20
configuration 14

D

disinfection 9–10
  -di qualifier 17
  data file 9–11
  program 9
  request for confirmation 17
disk space insufficient 35

E

error codes 11
  extended 17
executables
  UNIX 21
  Windows/DOS 18

F

filesystem
  scanning 6
  scanning starting filesystem only 15
full scan 18

I

icheckd.conf 28
IDEs
  specifying location 18
infected items
  disinfection 9, 17
  removal 19
InterCheck Server
  configuring 28–29
  monitoring 27
  reporting levels 30–31
  starting 27
  stopping 27

M

mailbox scanning 19
MIME files, scanning 18

Q

quarantine 21

R

recursive scan 19
removing Sophos Anti-Virus 40
reporting levels 30–31

S

scanning 6–7
  a directory or file 6
  a filesystem 6
  all file types 14
  archives 14, 16
  boot sector 7
  CD boot image 23
  compressed files 20
  default settings 6
  excluding items 17
  full scan 18
  local computer 6
  mailboxes 19
  MIME files 18
  options 14
  recursive 19
  runs slowly 35
  special objects 22
  starting filesystem only 15
screen output, copy to file/device 19
special objects
  exempting from scanning 22

sweep
  command line options 16
sweepic.ini 30
symbolically linked items
  scanning 21

U

uninstalling Sophos Anti-Virus 40
UNIX executables
  scanning 21

V

virus
  checking 6–7
  eliminating 9–10
  fragment reported 37
  reporting by clients 26–27
  warning 7

W

Windows/DOS executables
  defining for scanning 18
  exempting files from scanning 18

Z

zip bombs 18

Technical support

For technical support, visit

www.sophos.com/support

If you contact technical support, provide as much information as possible, including Sophos software version number(s), operating system(s) and patch level(s), and the exact text of any error messages.

Copyright 2002–2007 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.